George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama 35812

QD-QE-011
REVISION C
EFFECTIVE DATE: September 24, 2004

ORGANIZATIONAL INSTRUCTION

Software Quality Assurance Software Audits

OPR(s)	OPR DESIGNEE
QD10,QD20,QD30,QD40	Rosalynne Strickland

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Baseline		10/13/00	
Revision	A	9/09/02	Format and numbering change to implement requirements of QD-A-001 rev F.
Revision	B	09/18/03	Changes made to incorporate new QD40 organizational name
Revision	C	09/24/04	Revised to bring document in compliance with the HQ Rules Review Action (CAITS: 04-DA01-0387). Changes were also made to reflect S&MA organizational name changes (i.e., QS to QD).

Software Quality Assurance Software Audits

1.0 PURPOSE, SCOPE, AND APPLICABILITY

1.1 Purpose - The growth in cost and importance of software to NASA has caused NASA to address the improvement of software development across the agency. This organizational instruction describes the software quality assurance audits used at MSFC, in a way that is compatible with practices imposed by the agency.

1.2 Scope - It is the intent of this organizational instruction to further define audits, describe the audit process, and provide a tailorable checklist for use in an audit.

1.3 Applicability - This organizational instruction is applicable to Safety, Reliability, and Quality Assurance Policy and Assessment Department (QD40) associated with software quality assurance. This organizational instruction is written for the software quality assurance representatives who will perform audits.

2.0 DOCUMENTS (Applicable and/or Reference)

2.1 Applicable Documents

QD-QE-008	SOFTWARE ASSURANCE STATUS REPORT

2.2 Reference Documents

QD-QE-009	SOFTWARE ASSURANCE REVIEW/APPROVAL OF TECHNICAL DOCUMENTS

3.0 DEFINITIONS

3.1 Audit - refers to an SQA technique that is used to examine the conformance of a development process to procedures and the conformance of products to standards. An SQA audit also can examine the conformance of the actual status of the development activity to the reported status.

3.2 Procedures - the established criteria to which the development and control processes are compared. Procedures are the step-by-step directions that are to be followed to accomplish some development or control process.

3.3 Standards -the established criteria to which software products are compared. Software standards include documentation standards, design standards, and coding standards.

4.0 INSTRUCTIONS

An SQA audit has four phases: planning and preparation, the site visit, reporting, and follow-up. The interviews are conducted, and records and products are examined during the site visit. The reporting phase consists of the exit debriefing of the audited project, the preparation of a written report on the audit, and clarifying issues and providing related information as needed. Follow-up is done by the project, as the problems and deficiencies found in the audit are remedied. Follow-up may include re-auditing to assess the adequacy of the remedies.

4.1 Audit Planning and Preparation. - During the planning and preparation phase, the SQA auditor gains an understanding of the project. Based on the scope of the audit, the SQA auditor determines the specific questions that need to be answered, as well as the persons to be interviewed and the records and products to be examined to answer the questions. The SQA auditor examines records to see if a procedure is being correctly followed. Record examination is described below in terms of the principal processes that SQA audits examine: SCM, PRACA, and V&V. Similar activities would be used in the examination of other sets of records. Adequate notification of audits should be provided to the software developers for a number of reasons. Unannounced (surprise) audits are disruptive and demoralizing to the development staff and should be avoided. The intent of an audit program should be to help promote conformance with standards and procedures and the reporting of accurate status, not to "catch in the act" those "guilty" of violations. An announced schedule of audits allows proper preparation in terms of having required documentation available and being prepared to answer the SQA auditor's questions. There are 4 areas audited by SQA:

4.1.1 Software Configuration Management (SCM) Audit - During an audit of SCM, the SQA auditor shall examine the complete change control cycle, beginning with the initial processing of a change request; through analysis of impact and dispositioning; design, code, and testing; updating of documentation; submission of the modified products to the library; and closure of the change request. Records to be examined include the change requests as processed by the Change Control Board, the work authorizing documents issued as a result of approved changes, the code and documentation products that are intended to reflect the approved changes, and the program library records that capture the changes to code and data. Throughout the audit, the SQA auditor should be alert for and document any evidence of unauthorized changes. The records should show the authorization of each change, the product(s) to be changed, and the version numbers of the changed product. The SQA auditor shall check the products in the library to ensure that documentation is up-to-date with code changes. The SQA auditor shall check the version numbering and identification schemes, and the control documents. The records should demonstrate that there are adequate security measures in place to prevent loss and unauthorized changes.

4.1.2 Problem Reporting & Corrective Action (PRACA) Audit - When auditing the PRACA system, the SQA auditor shall examine the complete cycle. The SQA auditor shall review the software problem reports that are filed to assure that they are completely and correctly filled out. The disposition process and board actions should be recorded, usually on the same form. The nonconformances that result in product changes should be tracked to the product, and evidence should be gathered that changes are made, tested or reviewed, and approvals for issuance are granted. The SQA auditor should pay particular attention to corrected products to assure that they still satisfy requirements and standards.

4.1.3 Verification & Validation (V&V) Audit - An audit of V&V procedures should include a check of the verification matrix or equivalent, to assure that every requirement has a test and every test checks a requirement. Test plans should specify the test environment, test procedures, and the expected results for each test. Test procedures should be clear and detailed. Test plans and procedures should be reviewed and approved. The SQA auditor shall verify that test procedures were followed and that all nonconformances observed during testing are recorded in the PRACA system. In addition to testing, the SQA auditor shall assess other methods of V&V, if used. For example, if inspections or another form of peer reviews are used to find problems, the SQA auditor should verify that the records of the review show that they were done and that corrections and changes agreed to in the review are made in the product.

4.1.4 Product Examination - The intent of examination of products is two-fold: to see if standards are being followed and to see if status is accurately reported. Documents are measured against documentation requirements to make sure that all required documents exist, and against documentation standards to ensure that they have the correct content and style. The SQA auditor must read enough of the documents to form an opinion on the above; that is, the SQA auditor must be able to determine that a document presented as showing the design indeed contains design information. On the other hand, the SQA auditor is not responsible for the technical correctness of the documents and should not spend time trying to ascertain if the documents are correct. Code also is examined to determine if it meets standards. Code standards are likely to include rules for internal documentation, size of modules, styling formats, and other such items that the SQA auditor can verify. Rules for coding constructs or variable naming conventions are more difficult to verify. If the project has a code standards checker, the SQA auditor may run it on some code. If the standards checker is to be run at a certain step in the development process, or if peer reviews are used to verify coding standards, the SQA auditor must have access to those records. Products also are examined to compare their status with that reported. Documents reported as complete, for example, should contain all of the sections given in the table of contents (which may be prescribed by a documentation standard), should be signed by the approving authorities, and should contain few, if any, To-Be-Determined (TBDs) items. Code implementation usually goes through the steps of detailed design, code, peer review, and unit test. A module that is reported as complete should have gone through all of the above steps, should meet the coding standards, and should have whatever approvals are required. The Unit Development Folder or equivalent should contain all of the evidence to look at status of coding.

4.2 The Site Visit - The purpose of the audit site visit is to collect the data necessary to assess that the required products are being produced, the degree to which they conform to applicable standards, how well procedures are being followed, and that the reported status corresponds to the actual status. The audit is intended to uncover any significant deviation from standards, procedures, or reported status so that corrective action can be taken. The SQA auditor uses two basic techniques: interviews with project staff and examination of documentation and records.

4.2.1 Entrance Briefing - The site visit should begin with an entrance briefing, involving the SQA auditor and key project staff. During this briefing, the SQA auditor should describe the focus of the audit, and identify the interviews to be conducted and the records to be examined. The entrance briefing may also be used by the project to brief the SQA auditor on its processes, key staff members, and current status. Time for questions and answers should be included. The SQA auditor should assure the project that an exit interview would be held where the SQA auditor will present preliminary findings to the project and the project may provide any additional information to the SQA auditor. After the entrance briefing, the SQA auditor should proceed with the gathering of information.

4.2.2 Gathering of Information - It is useful to begin the information gathering process with interviews, during which the SQA auditor tries to understand the realities behind the documented plans and procedures. The SQA auditor should learn which individuals carry out a procedure, approve a change or fix, keep project records, etc. Each individual should be asked to describe their perceptions of and interactions with the process. The SQA auditor should take notes, annotate or develop procedural flow diagrams, ask questions to clarify, and make it their objective to clearly understand the process. In particular, the SQA auditor should be alert for indications of shortcuts or abbreviations to the procedure. During interviews, the SQA auditor must remember that data is being gathered, and that conclusions should wait until all of the facts are in. This provides a clearer understanding of the actual processes used on the project and eases communications with the staff. The checklist developed during the preparation phase is used to guide the discussions during the interview.

4.2.2.1 Preparing a Checklist – An audit checklist is a list of items that the SQA auditor intends to examine and questions the SQA auditor intends to ask during the site visit portion of the audit. While a generic checklist may be used as a basis for all audits, better results will be achieved if the generic checklist is tailored for each audit. Tailoring consists of choosing appropriate items or questions from the generic checklist, expanding the level of detail, adding additional questions and topics, and changing the wording of the questions to fit the project's nomenclature. Information for tailoring may come from the contract requirements, organizational standards and practices, and results and action items from previous audits. A sample generic checklist is provided in Appendix A. To tailor this checklist, the SQA auditor should determine whether questions should be answered by interviews, examination of the software products and documents, examination of records, or a combination of methods. As much as possible, questions should be phrased in terms of the specific project and organization being audited, and should use the names and terms that the project uses. The form should, if possible, allow the checking of boxes or simple entry of information. As the SQA auditor proceeds with the site visit, the checklists and forms can be completed with the information obtained. The SQA auditor must retain the flexibility to modify the forms or questions as information is gathered. Additional questions are likely to be suggested by answers given, and forms may not have been properly made in advance to record the real situation. It is important to remember that the checklist and forms derived from it are guides, and that the objective of the audit is to understand and report on the actual state of affairs in the developing organization.

Once the SQA auditor is sure that the processes and procedures are understood as they really exist, they should begin examining the tangible parts of the project: its products and records. Products consist of requirements and design documentation, including unit development folders, user manuals, code, etc. Records consist of memoranda and forms that document the events in the life of a product. They come from SCM, PRACA, and V&V, among others.

4.3 Audit Reporting - Once the interviews and record examination have been completed, initial results should be shared with the staff of the audited project during an exit interview. The exit interview provides an opportunity to clear up misunderstandings and allows project office to present any information that they feel the SQA auditor failed to consider. In addition, the project learns immediately about the problems that have been found and can begin making plans to correct them. After adjusting the initial results to reflect the information gathered in the exit interview, the SQA auditor prepares a written final report. The report should be organized to highlight the most significant results, addressing both problems and commendations, and should include a general narrative of the audit. The audit report should be in accordance with organizational instruction QD-QE-008. The objective of the audit report is to present a clear picture of the status of a development activity or a facet of the activity to project management. The report must be clear, objective, and factual. In some cases, the SQA auditor will find that, while procedures are being followed or standards are being met, the procedures or standards are not effective in producing a quality product. It is the responsibility of the SQA auditor to note the specific problems caused by the procedure and/or standard and include them in the report. In general, however, problems that the SQA auditor identifies should be related to project or contractually required procedures and standards; the SQA auditor's opinion of their desirability should not affect their evaluation of the adherence to them.

4.4 Audit Follow-up - While the SQA auditor's role is essentially finished after producing the audit report, actions to resolve deficiencies identified in that report, must be taken by the project office. Problems that are feasible and reasonable to correct should be converted to action items and assigned to appropriate individuals. A rationale should be developed for those that are not to be corrected. It is the responsibility of the software developers to improve their processes in response to deficiencies identified by the audit. The changes should be tracked to ensure they occur and are effective and the closure of action items should be documented. In many cases, the best way to determine if the problems have been solved is through a follow-up audit.

5.0 NOTES

None

6.0 SAFETY PRECAUTIONS AND WARNING NOTES

None

7.0 APPENDICES, DATA, REPORTS, AND FORMS

Appendix A, Listing of SQA audit questions that can be tailored for an audit.

8.0 RECORDS

None

9.0 TOOLS, EQUIPMENT, AND MATERIALS

None

10.0 PERSONNEL TRAINING AND CERTIFICATION

None

11.0 FLOW DIAGRAM

None

12.0 RESPONSIBILITIES

Work accomplished within the scope of this organizational instruction will be performed by the Software Assurance representative. The Safety, Reliability, and Quality Assurance Policy and Assessment Department (QD40) may delegate the responsibilities and tasks provided in this organizational instruction to support contractors who are responsible for carrying out the tasks identified herein.

Appendix A

The following is a list of questions that can be tailored for an SQA audit. Questions appropriate to a specific audit should be selected and then modified to reflect local terminology or procedures. The questions should be placed on a form that allows space for recording answers.

Software Development Documentation

Are standards for preparation of deliverable documentation established?
Does the documentation meet the standards?
Are procedures established and documented to assure that standards are followed?
Do the procedures address the changes to software documentation that are placed under configuration management control?
Are the changes reviewed in the same manner as the base document?
Are methods established for traceability of documentation, including changes?
Are the contents of deliverable documents clear, concise, complete, and understandable?
Are procedures established to enforce consistency in writing?
Are review teams familiar with the material being reviewed to detect inconsistency?
Is approval authority for deliverable documentation clearly stated?
Is required documentation provided to the customer in a timely, responsive manner?
Are sufficient copies furnished?
Are established procedures followed in the production of both deliverable and non-deliverable documents?
Does the documentation in the development folder match the phase of the life cycle?
Does the level of detail in documentation look reasonable?

Code

Do code, prolog, and Program Design Language (PDL) adhere to all prevailing standards and conventions?
Are necessary elements of the prolog complete; e.g., are all data elements described, all subroutines defined?
Is internal code documentation present in amounts required by standards?
Is the code consistent with its design, as presented in its prolog and PDL?
Does the code appear to be correct for test cases that can be verified by a quick, visual inspection?
Is all debugging code clearly identified?
Are all stubs and test files identified?
Do test cases appear adequate based on the PDL?

Software Configuration Management

Has a software configuration management (SCM) plan been developed?
Has the plan been baselined?
Provided to the acquirer?
Are SCM instructions for identification of baseline items and subsequent revision or versions being followed?
Are SCM procedures in place, which require approval authority for adding and removing items in the program library?
Is the SCM organization adequately staffed, fully funded, and responsive? Are responsibilities clearly understood?
Do baseline documents comply with contract requirements?
Do the approved specifications serve as a baseline for control of changes?
Is a list of approved specifications maintained? Current?
Changes posted?
Are procedures established for the production of software documentation adequate and rigidly enforced?
Are procedures for handling problem reports adequate and efficient?
Has a Configuration Control Board (CCB) been established? Who are the members? Is SQA represented? Do all members attend regularly? Are CCB actions handled in a timely manner? Are agenda and minutes published? Are CCB action items followed up?
Are SCM status accounting documents maintained? Are they current?
Does the SCM plan address configuration audit?
Have formal configuration audits been conducted or planned (including FCA and PCA)?

Computer Program Library

Has a Computer Program Library been established? A program librarian appointed?
Have adequate procedures been identified for: Library controls?; Configuration item controls?; Problem report handling?
Is the program librarian complying with established procedures?
Are problem reports implemented into appropriate development folders?
Are computer program versions accurately identified, controlled, and documented through the life cycle? Is an automated source control system used? Is it adequately maintained?
How is the library controlled (error report, change request, etc.)?
Are only authorized/approved modifications made to source and object programs released to the library? How is it controlled (error report, change request, etc.)?
What measures are being taken to assure all approved modifications are properly integrated and that software submitted for testing is the correct version?

Is non-deliverable software monitored and controlled to the extent specified in the development plan?
Are development folders regularly submitted to the program librarian?
Does a library documentation index exist? Is it current?
Does a log exist showing what material has been checked in and out of the library? Does it appear accurate?
Does all submitted code include proper transmittal information?
Is this available for review?
Is documentation updated to correspond with newly submitted code?
Are all items placed in the program library assigned an identification number related to the version number? Does this number relate to the associated documentation?
Is the flow through a change cycle clear, efficient, documented, and correct? (Test several samples.)

Problem Reporting and Corrective Action

Have procedures assuring prompt detection and correction of deficiencies been established?
Are data analyzed and problem and deficiency reports examined to determine extent and causes?
Are trends in performance of work analyzed to prevent development of nonconforming products?
Has corrective action been documented accurately on problem reports?
Has corrective action been reviewed and monitored to determine adequacy, effectiveness, and whether contract requirements are being met?
Are all corrective action reports and analyses on file?
Is there management support for the corrective action system?
Is the program librarian following procedures for maintaining control and status of problem reports?
Are discrepancies generated by non-deliverable computer programs treated the same as those for deliverables?
Are problem reports pertaining to a unit contained within the development folder for that unit?
Are the software developers complying with the requirement to generate problem reports during integration?
Is there documented approval for all changes to items under configuration control? Do all forms have required signatures?

Verification and Validation

Have the software requirements been analyzed to determine testability?
Are test objectives adequate, feasible, and sufficient to demonstrate software performance to meet contractual requirements? Do project personnel understand them?
Are the test philosophy and methodology based on assumptions that are acceptable to SQA? Is there a procedure to monitor assumptions and a way to alert the test director if an assumption is unacceptable?

Do test plans and procedures comply with specified standards and contractual requirements?
Are the test plans and procedures approved by the customer, where required?
Are all test tools and equipment identified, defined, calibrated, and controlled prior to testing the software? Is all necessary test hardware certified (both computer and ancillary)?
Is software baselined prior to testing?
Is the correct version of software and associated documentation certified prior to testing?
Does an SQA representative monitor acceptance testing? By the customer, when required? If not, then who monitored the tests?
Are tests conducted according to approved test plans and procedures?
Have test results been certified by participating members to reflect the actual test findings?
Have test reports been reviewed and certified? By whom? Are deficiencies documented in problem reports?
Has test-related documentation been maintained and controlled to allow repeatability of tests?
Is there a test verification matrix to assure all requirements are tested? Does it look reasonable?
Are test procedures clear and repeatable?
Do actual and expected test results match? If not, has a problem report been filed?

Project Status

Do completion dates in development folders/status sheets agree with status report to management? If not, how great is the difference?
According to the development/management plan, the project where it should be? What activities should be current? How should the project be staffed? What intermediate projects should be delivered? What reviews or milestones should have occurred?
Where does the project actually stand now? Determine:

- Current phase
- Activities levels
- Staff composition
- Documents delivered
- Milestones reached
- Results of reviews